IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1–104. (Canceled)

105. (Currently Amended) A computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein the program is running on an operating system of the computer system; and

executing each of a first and a second plurality of detection routines on the operating system of the computer system, wherein the first plurality of detection routines are executable to determine whether the selected code under investigation has characteristics and behaviors usually associated with a valid program, wherein the second plurality of detection routines are executable to determine whether the selected code under investigation has characteristics and behaviors usually associated with a malicious program, and wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results; and

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code~~, wherein the second score is obtained independently of the first score~~; and

upon completing the executing of the first and second plurality of detection routines, using at least one of the first and second scores to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system.

106. (Canceled)

107. (Currently Amended) The method of claim 105, wherein said method is performed repeatedly until a plurality of active programs on the computer system have been categorized with respect to their likelihood of compromising the security of the computer system ~~further comprising:~~

~~after categorizing the selected active program, selecting, in turn, each of a plurality of additional active programs on the computer system as code under investigation, wherein each of the plurality of additional active programs is running on the operating system of the computer system; and~~

~~executing each of the first and second plurality of detection routines on the operating system of the computer system with respect to said selected code under investigation~~.

108. (Canceled)

109. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect remote control software.

110. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a keystroke logger.

111. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect spyware.

112. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a worm.

113. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a virus.

114. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect monitoring software.

115. (Currently Amended) A computer-implemented method comprising:

selecting code currently running on a computer system as code under investigation, wherein said code is running on an operating system of said computer system; and

executing each of a first and a second plurality of detection routines on the operating system of the computer system, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results; and

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code, wherein the second score is independent of the first score; and

upon executing each of the first and second plurality of detection routines:

using at least one of the first and second scores to categorize the code under investigation into one of a plurality of categories, including first and second categories indicative of valid code and malicious code, respectively;

wherein the first and second pluralities of detection routines each include at least one routine executable to determine a characteristic of the code under investigation and at least one routine executable to determine a behavior of the code under investigation.

116. (Canceled)

117. (Previously Presented) The method of claim 115, wherein at least some of the code associated with the selected active code is running in kernel mode.

118. (Previously Presented) The method of claim 115, further comprising:

selecting additional active code as code under investigation; and

executing each of the first and second pluralities of detection routines with respect to said selected code under investigation.

119-126. (Canceled)

127. (Currently Amended) A computer system comprising:

a processor; and

a memory storing program instructions executable by the processor to:

select a program currently running on a computer system as code under investigation, wherein said program is running on an operating system of said computer system; and

execute each of a first and a second plurality of detection routines on the operating system of the computer system, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation is valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results; and

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation is malicious code; and

upon completing execution of the first and second plurality of detection routines, use at least one of the first and second scores to make a determination whether the code under investigation represents a security threat to the computer system;

wherein the first and second pluralities of detection routines each include at least one routine executable to determine a characteristic of the code under investigation and at least one routine executable to determine a behavior of the code under investigation.

128. (Currently Amended) A computer-readable ~~memory~~ storage medium having stored thereon~~, including~~ program instructions that are ~~computer~~ executable by a computer system to:

select a program currently running on an operating system of the computer system as code under investigation; and

execute each of a first and a second plurality of detection routines on the operating system of the computer system, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results, wherein the first plurality of detection routines includes at least one routine executable to test for ~~at least one of the following:~~ a characteristic[[s]] typically associated with valid code and at least one routine executable to test for a behavior[[s]] typically associated with valid code;

weighting and combining each of the first plurality of results to obtain a first composite score;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results, wherein the ~~first~~ second plurality of detection routines includes at least one routine executable to test for ~~at least one of the following:~~ a characteristic[[s]] typically associated with malicious code and at least one routine executable to test for a behavior[[s]] typically associated with malicious code; and

weighting and combining each of the second plurality of results to obtain a second composite score; and

upon executing each of the first and second plurality of detection routines, use at least one of the first and second composite scores to make a determination whether the code under investigation is malicious code.

129. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is malicious code.

130. (Previously Presented) The method of claim 129, wherein the malicious code does not have a known signature.

131-132. (Canceled)

133. (Previously Presented) The method of claim 105, wherein the malicious code is a previously unknown type of malicious code.

134. (Previously Presented) The method of claim 129, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

135. (Previously Presented) The method of claim 105, wherein the determination is made from the first and second scores that the code under investigation is valid code.

136. (Previously Presented) The method of claim 105, wherein the determination is made that the code under investigation is valid code, wherein the determination is made based on the first score exceeding a valid code threshold value, regardless of the second score.

137. (Previously Presented) The method of claim 105, wherein the determination is made that the code under investigation is valid code, wherein the determination is made based on the first score exceeding a valid code threshold and the second score not exceeding a malicious code threshold.

138. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code.

139. (Currently Amended) The computer system of claim 127, wherein the program instructions are executable by the processor to:
determine from the first and second scores that the code under investigation is malicious code.

140. (Currently Amended) The computer system of claim 139, wherein the malicious code is a previously unknown type of malicious code.

141. (Currently Amended) The computer system of claim 139, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

142. (Currently Amended) The computer system of claim 127, wherein the program instructions are executable by the processor to:

determine from the first and second scores that the code under investigation is valid code.

143. (Currently Amended) The computer system of claim 142, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value, regardless of the second score.

144. (Currently Amended) The computer system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is suspicious code.

145. (Currently Amended) The ~~memory~~ storage medium of claim 128, wherein the program instructions are executable by the computer system to:
determine from the first and second scores that the code under investigation is malicious code.

146. (Currently Amended) The ~~memory~~ storage medium of claim 145, wherein the malicious code is a previously unknown type of malicious code.

147. (Currently Amended) The ~~memory~~ storage medium of claim 128, wherein the program instructions are executable by the computer system to:

determine from the first and second scores that the code under investigation is valid code.

148. (Currently Amended) The ~~memory~~ storage medium of claim 147, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value, regardless of the second score.

149. (Currently Amended) The ~~memory~~ storage medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code.

150. (Currently Amended) The ~~memory~~ storage medium of claim 145, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

151. (Previously Presented) The method of claim 105, wherein at least some of the code associated with the selected active program is running in kernel mode.

152. (Currently Amended) One or more computer-readable storage media having stored thereon ~~storing~~ program instructions executable on a computer system to:

while a first program is running on an operating system of the computer system:

execute each of a first and second plurality of detection routines on the operating system of the computer system to gather information about the first program, including characteristics and behavior~~sal information about~~ of the first program, wherein ~~various ones of~~ the first plurality of detection routines are executable to detect characteristics and behaviors indicative of valid code, and wherein ~~various ones of~~ the second plurality of detection routines are executable to detect characteristics and behaviors indicative of malicious code;

upon completing execution of each of the first and second plurality of detection routines:

use the results of the first plurality of detection routines to determine a first value indicative of the likelihood that the first program is valid code;

use the results of the second plurality of detection routines to determine a second value indicative of the likelihood that the first program is malicious code;

use at least one of the first and second values to determine whether the first program is a security threat to the computer system.

153. (Currently Amended) The computer-readable storage media of claim 152, wherein the program instructions are executable to determine whether the first program is a security threat to the computer system based on a first comparison between the first value and a valid code threshold value and also based on a second comparison between the second value and a malicious code threshold value.

154. (Currently Amended) The computer-readable storage media of claim 152, wherein the program instructions are executable to determine that the first program is a security threat to the computer system based on the first value not exceeding a valid code threshold value and on the second value exceeding a malicious code threshold value.

155. (Currently Amended) The computer-readable storage media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to

the computer system based on the first value exceeding a valid code threshold value, regardless of the second value.

156. (Currently Amended) The computer-readable storage media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to the computer system based on the first value exceeding a valid code threshold value and on the second value not exceeding a malicious code threshold value.

157-158. (Canceled)

159. (Currently Amended) A method, comprising:

while a first program is running on an operating system of a computer system, executing each of a first and second plurality of detection routines on the operating system of the computer system, wherein ~~various ones of~~ the first plurality of detection routines includes routines that are executable to determine behaviors of the first program that are indicative of valid code, and wherein ~~various ones of~~ the second plurality of detection routines includes routines that are executable to determine behaviors of the first program that are indicative of malicious code;

using results of the first plurality of detection routines to compute a first ~~score~~ value indicative of the likelihood that the first program is valid code;

using results of the second plurality of detection routines to compute a second value indicative of the likelihood that the first program is malicious code;

using at least one of the computed first and second values to categorize the first program as to the likelihood of the first program compromising the security of the computer system.

160-161. (Canceled)

162. (Previously Presented) The method of claim 159, wherein said using at least one of the computed first and second values includes performing comparisons involving the first and second values.

163. (Currently Amended) The method of claim 162, wherein said first program is categorized based on a comparison between the first value ~~score~~ and a valid code threshold.

164. (Currently Amended) The method of claim 163, wherein the first program is categorized as not being a security threat based on the first value ~~score~~ exceeding the valid code threshold, regardless of the second score.

165. (Currently Amended) The method of claim 162, wherein said first program is categorized based on a comparison between the first value ~~score~~ and a valid code threshold and also on a comparison between the second value ~~score~~ and a malicious code threshold.

166. (Currently Amended) The method of claim 165, wherein the first program is categorized as not being a security threat based on the first value ~~score~~ exceeding the valid code threshold and the second ~~score~~ value not exceeding the malicious code threshold.

167. (Canceled)

168. (Previously Presented) The method of claim 105, wherein each of the detection routines within the first and second plurality of detection routines gathers a different type of information about the code under investigation, and wherein the first and second pluralities of detection routines are not themselves running on the operating system of the computer system in a manner that prevents the code under investigation from infecting the computer system.

169. (Previously Presented) The method of claim 105, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that, when executed, obtains information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

170. (Canceled)

171. (Previously Presented) The method of claim 115, wherein each of the detection routines within the first and second plurality of detection routines gathers a different type of information about the code under investigation, and wherein the first and second pluralities of detection routines are not themselves running on the operating system of the computer system in a manner that prevents the code under investigation from infecting the computer system.

172. (Previously Presented) The method of claim 115, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that, when executed, obtains information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

173. (Canceled)

174. (Previously Presented) The computer system of claim 127, wherein each of the detection routines within the first and second plurality of detection routines is executable to gather a different type of information about the code under investigation, and wherein the first and second pluralities of detection routines do not execute on the operating system of the computer system in a manner that prevents the code under investigation from infecting the computer system.

175. (Previously Presented) The computer system of claim 127, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that is executable to obtain information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

176. (Canceled)

177. (Currently Amended) The computer-readable ~~memory~~ storage medium of claim 128, wherein each of the detection routines within the first and second plurality of detection routines is executable to gather a different type of information about the code under investigation, and wherein the first and second pluralities of detection routines do not execute on the operating

system of the computer system in a manner that prevents the code under investigation from infecting the computer system.

178. (Currently Amended) The computer-readable ~~memory~~ storage medium of claim 128, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that is executable to obtain information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

179. (Canceled)

180. (Currently Amended) The computer-readable ~~memory~~ storage media of claim 152, wherein each of the detection routines within the first and second plurality of detection routines is executable to gather a different type of information about the first program, and wherein the first and second pluralities of detection routines do not execute on the operating system of the computer system in a manner that prevents the first program from infecting the computer system.

181. (Currently Amended) The computer-readable ~~memory~~ storage media of claim 152, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that is executable to obtain information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

182. (Currently Amended) The computer-readable ~~memory~~ storage media of claim 152, wherein the program instructions are further executable, for each of a plurality of additional programs running on the operating system of the computer system, to:

execute each of the first and second pluralities of detection routines on the operating system of the computer system relative to that additional program;

use results of the execution of the first and second pluralities of detection routines to determine whether that additional program is a security threat to the computer system.

183. (Previously Presented) The method of claim 159, wherein each of the detection routines within the first and second plurality of detection routines gathers a different type of information

about the first program, and wherein the first and second pluralities of detection routines are not themselves running on the operating system of the computer system in a manner that prevents the first program from infecting the computer system.

184. (Previously Presented) The method of claim 159, wherein there is at least one detection routine within the collective first and second pluralities of detection routines that, when executed, obtains information about the code under investigation by accessing the operating system of the computer system via an API of the operating system.

185. (Previously Presented) The method of claim 159, further comprising:

for each of a plurality of additional programs running on an operating system of the computer system:

execute each of the first and second pluralities of detection routines on the operating system of the computer system relative to that additional program;

use results of the execution of the first and second pluralities of detection routines to categorize that additional program as to the likelihood of that additional program compromising the security of the computer system.